Política: Clasificación de la Información

Código: PL-DTI-005	**Fecha de vigencia**: dd/mm/aaaa
Versión: 1.0	**Fecha de última actualización**: dd/mm/aaaa

1. Objetivo

Clasificar la información en el COSEVI para garantizar que recibe el nivel de protección adecuado.

2. Alcance

Esta política es aplicable a todos los funcionarios del COSEVI, terceros y usuarios de los recursos de tecnología de información.

3. Responsables

Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

Dueños de los datos: Identificar y clasificar la información, con el fin de asegurar que reciba un apropiado nivel de protección según su sensibilidad y criticidad, de acuerdo con la metodología establecida por la Dirección de TI.

Comité Gerencial de TI: Actuar en relación con sus funciones con respecto a lo estipulado en esta política.

Dirección de TI: Liderar el proceso de clasificación de la información.

Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

4. Pautas

4.1 La información debe ser clasificada en función de su valor, sensibilidad y criticidad para el COSEVI.

4.2 La clasificación de la información debe permitir establecer diferencias entre las medidas de seguridad a aplicar que, de forma general, atenderán a criterios de disponibilidad, integridad y confidencialidad de los datos.

4.3 La Dirección de TI debe definir un método para la clasificación de la información donde se definan las categorías a utilizar. Para esta definición se deben tomar en cuenta las diferentes Direcciones del COSEVI.

4.4 El método para la clasificación de la información a definir deberá tomar en cuenta la cantidad de categorías de clasificación, los esquemas demasiado complejos pueden volverse engorrosos y resultar siendo más costosos o poco prácticos.

4.5 El método de clasificación de la información debe considerar información impresa o digital, independientemente del tipo de almacenamiento o medio de transferencia.

4.6 Los dueños de los datos deberán realizar seguimiento a la información que tienen bajo su custodia para detectar cambios que se puedan realizar al nivel de clasificación. Si se detecta algún cambio deben informar a la Dirección de TI para tomar las medidas respectivas.

4.7 Los dueños de los datos en conjunto con su jefatura deberán establecer los requisitos que deberán cumplir las personas que requieran acceso a la información de acuerdo con la clasificación.

4.8 Se deberá considerar los requerimientos especiales para el acceso a la información, ya sean estos acuerdos de confidencialidad o no revelación, entre otros.

4.9 La Dirección de TI en una labor conjunta con las Direcciones del COSEVI, deben definir revisiones periódicas del método de clasificación de la información.

4.10 La Dirección de TI debe coordinar en conjunto con el Departamento de Gestión y Desarrollo Humano la educación de los funcionarios del COSEVI para inculcar el compromiso de proteger la información de acuerdo con su clasificación.

4.11 La Dirección de TI debe identificar y divulgar los roles y las responsabilidades para la manipulación de la información (dueño de la información, custodio de la información y usuarios de la información)

4.12 La Dirección de TI debe desarrollar los procedimientos establecidos para la revisión del método de clasificación de la información, los cuales deben incluir la valoración de las necesidades del negocio para compartir y restringir la información, las obligaciones legales en caso de que existan y el nivel de impacto asociado.

4.13 Toda información clasificada debe ser rotulada. La etiqueta debe reflejar su clasificación. Esto aplica para reportes impresos y en pantalla, medios de almacenamiento (cintas magnéticas, discos, llaves mayas), mensajes electrónicos y archivos transferidos.

4.14 Se debe manejar métodos para etiquetar activos de la información en formato físico y electrónico.

4.15 Los dueños de los documentos impresos, digitalizados y electrónicos, así como las personas que los manipulen, son responsables de mantenerlos seguros de acuerdo con el método de clasificación definido.

4.16 Los acuerdos con otras organizaciones que compartan información con el COSEVI, deben incluir procedimientos para identificar la clasificación de dicha información e interpretar la marca de clasificación de otras organizaciones.

4.17 Información sensible del COSEVI no debe encontrarse en mensajes de voz internos o externos o dispositivos de almacenamiento externo, salvo casos en los que sea estrictamente necesario y justificados.

5. Sanciones

El incumplimiento de esta política constituye una falta grave según lo establecido por el Reglamento Autónomo de Organización y Servicio del Consejo de Seguridad Vial.

6. Aprobación

6.1 Aprobación y dictamen de conformidad técnica de la DTI

Nombre	Puesto	Firma
	Dirección de TI	

6.2 Aprobación por la Junta Directiva

Acuerdo de aprobación por Junta Directiva	

7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión